Incident report analysis

Summary	Company experienced a security incident when all network services stopped responding. The security team found out that it was caused by aDDoS attack by flooding network with ICMP packets. The team responded by blocking the attack and stopping all non critical network services.
Identify	Org experienced a DDos attack. Network stopped working due to incoming flood of ICMP packets. Internal network traffic could not access any network resources. The vulnerability was through an unconfigured firewall
Protect	Security team implemented a new firewall rule to limit the rate of incoming ICMP packets. Source IP address verification ont he firewall to check for spoofed IP addresses on incoming ICMP packets
Detect	We established a Network monitoring software to detect abnormal traffic patterns
Respond	As a response, a firewall rule was implemented. An IDS/IPS system was added and a monitoring system will be installed to contain and analyze security risks
Recover	We blocked all incoming ICMP packets to stop all non-critical network services online and then restoring critical network services

---

Reflections/Notes: